REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JULY 2009	Conference Paper Postprint	January 2009 – May 2009

4. TITLE AND SUBTITLE

RANKING ACTIVITIES BASED ON THEIR IMPACT AND THREAT

5a. CONTRACT NUMBER
In House

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62702F

6. AUTHOR(S)

John J. Salerno and George P. Tadda

5d. PROJECT NUMBER
459E

5e. TASK NUMBER
NO

5f. WORK UNIT NUMBER
E2

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AFRL/RIEA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIEA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2009-35

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution unlimited PA# 88ABW-2009-2059

13. SUPPLEMENTARY NOTES
This paper was presented at the 12th International Conference on Information Fusion (Fusion 2009), Seattle, Washington, 6-9 July-2009. This is a work of the United States Government and is not subject to copyright protection in the United States.

14. ABSTRACT
Many say we live in the information age, but in reality if you ask any analyst today they would say we live in the data age. The amount of data being presented and displayed to the analyst is overwhelming – to a point that in many cases they are missing the salient of key activities of interest. Analysts are spending the majority of their time filtering through the data rather than performing analysis. Until recently, in the past five years, has there been an increased emphasis in higher level fusion or what many are calling situation awareness. So why the increased interest? In this paper we will look at this very issue, review our reference model and provide a discussion of a flow through the model to include how we can rank various activities based on their impact and threat.

15. SUBJECT TERMS
Impact Assessment, Threat Assessment, Situation Awareness, Knowledge of "Us", Knowledge of "Them", Intent, Opportunity.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John J. Salerno
U	U	U	UU	5	19b. TELEPHONE NUMBER (*Include area code)* N/A

Ranking Activities Based on Their Impact and Threat

John J. Salerno
Air Force Research Laboratory
Rome, NY USA
john.salerno@rl.af.mil

George P. Tadda
Air Force Research Laboratory
Rome, NY USA
george.tadda@rl.af.mil

Abstract – *Many say that we live in the information age, but in reality if you ask any analyst today they would say we live in the data age. The amount of data being presented and displayed to the analyst is overwhelming – to a point that in many cases they are missing the salient or key activities of interest. Analysts are spending the majority of their time filtering through the data rather than performing analysis. Until recently, in the past 5 years, has there been an increased emphasis in higher level fusion or what many are calling situation awareness. So why the increased interest? In this paper we will look at this very issue, review our reference model and provide a discussion of a flow through the model to include how we can rank various activities based on their impact and threat.*

Keywords: Impact Assessment, Threat Assessment, situation Awareness, Knowledge of "Us", Knowledge of "Them", Intent, Opportunity

1. Background

In earlier work we introduced a concept of the DIR, Data to Information Ratio. The idea behind this metric was to measure the amount of compression or reduction that can be achieved by aggregating events/objects into groups and activities. As an example, consider a military force, composed of a number of geographically disperse units and containing many vehicles. If we were to track and display all of these objects a typical display would be black from the density. If we were able to group these objects into clusters and identify these clusters as the units and display icons that represent them, the display would be much more understandable. A second example comes from the cyber side. An analyst is required to try to find a potential attack within thousands of alerts (pings, probes, etc.) However if there was a capability that could aggregate alerts together into what we call attack tracks, an analyst could be reviewing hundreds of tracks rather than the thousands of observations/alerts that they do today - but aggregation alone is not sufficient. We need to also provide a way to draw their attention to those that are important? This ranking or prioritization is done by assessing the impact (and thus the potential threat) that an ongoing activity may have on us, our assets or to the mission. So how do we define what an impact or threat is? What type of data, information or knowledge do we need to understand a given activity's impact or threat? In the remaining paragraphs we will attempt to define what we mean by an impact or threat, a process derived based on our reference model and the types of knowledge needed to support situation assessment and enable a decision maker's overall situation awareness.

2. Defining Impact/Threat Assessment

Impact and Threat have been addressed specifically by two different sets of researchers. Bosse, Roy and Wark [10] define Situation Assessment as "a quantitative evaluation of the situation that has to do with the notions of judgment, appraisal, and relevance." Two products or components of situation assessment are: Impact and Threat assessment. Impact assessment is defined as "the force of impression of one thing on another; an impelling or compelling effect. There is the notion of influence: one thing influencing another. In that sense, impact assessment estimates the effects on situations of planned or estimated/predicted actions by the participants, including interactions between action plans of multiple players." Bosse, Roy and Wark goes on further and defines threat assessment as "an expression of intention to inflict evil, injury, or damage. The focus of threat analysis is to assess the likelihood of truly hostile actions and, if they were to occur, projected possible outcomes…."

Steinberg [11] states that: "Threat Assessment involves assessing situations to determine whether detrimental events are likely to occur. Per the JDL Data Fusion Model, Threat Assessment is a level 3 data fusion process. Indeed, the original model [3] used 'Threat Assessment' as the general name for level 3 fusion; indicative of the importance of that topic. In subsequent revisions [4], the concept of level 3 has been broadened to that of Impact Assessment. Steinberg goes on to decompose threat into *capability*, *opportunity* and *intent* to be the principal factors in predicting (intentional) actions.

- *Capability* involves an agent's physical means to perform an act;

- *Opportunity* involves spatio-temporal relationships between the agent and the situation elements to be acted upon;
- *Intent* involves the will to perform an act.

In [7] we provided a set of definitions and a combined reference model based on many years of research in this area. The model, as shown in Figure 1, was built by combining the JDL Data Fusion model and Endsley's SA Model. As part of [7], we've refined how one can think of JDL Levels 1 and 2 as well as described differences between JDL Levels 2/3 and Endsley's idea of projection.

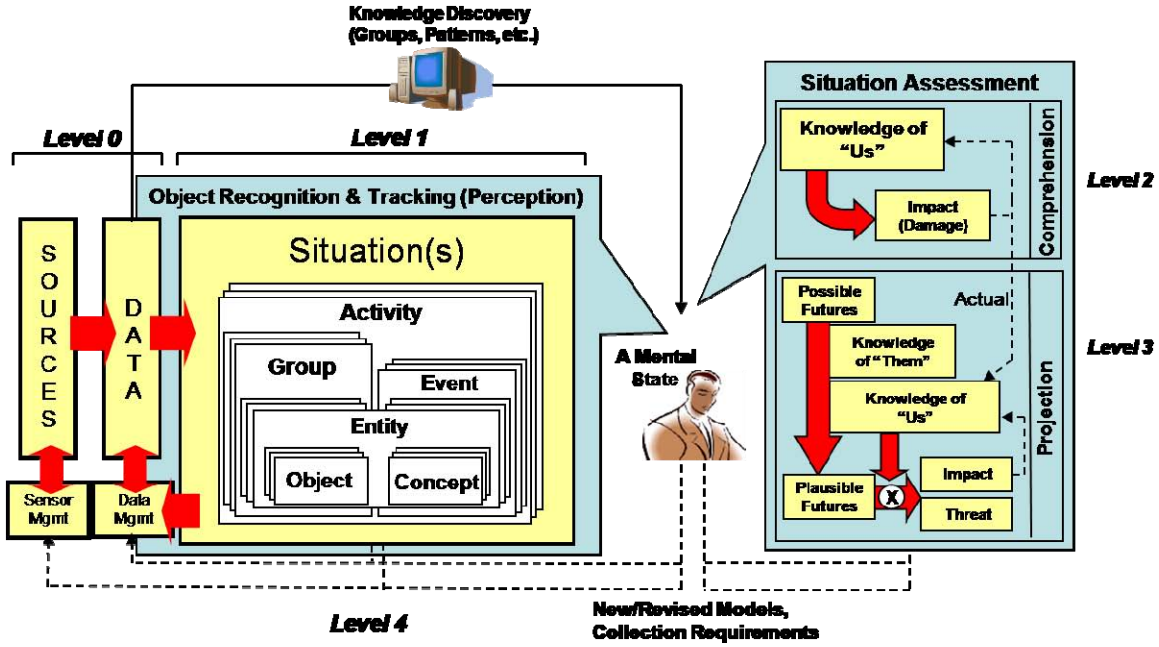

Figure 1 - Situation Awareness Reference Model

2.1. A Snapshot in Time

Figure 2 expands upon the reference model and looks at it as a process in an instance of time. Observables are the input to the process that provides a view of what is going on in the world (primitive elements of the environment). It is assumed that any attributes associated with the observables have been normalized, cleansed, and transformed into a form that can be used by the follow-on processes. The observables we are interested in are cues into the activities that a decision maker needs or is interested in (and thus we refer to these as Activities of Interest, AOI) as a way to gain or maintain awareness. The AOI are based on goals, policies, or in general the "things" of interest. These AOIs can be stored and manipulated in such formats as graphs, Bayesian networks, Markov models, or any of the numerous modeling techniques. As observables enter the process, they are categorized and (1) associated with a new stage or step within an existing, ongoing activity; (2) associated with no existing activity and hence become the start of a new activity; or (3) can be a trigger leading to the combination, merging, or removal of existing activities. The aggregation process is similar to tracking individual objects (as defined by JDL Level 1) and why we consider this part of the process, even though dealing with events, still Level 1. Objects are no longer a physical entity like a tank but an activity – a collection of events and observables. The classical tracking problem of association also comes in to play when associating an observable to an activity or step of an activity.

At any given time, say *t*, we have a set of ongoing activities (defined earlier as the current situation). At this point we are interested in analyzing the meaning of these activities. This is considered to be Situation Assessment (as shown on the right side of the reference model in Figure 1). The overall objective of Situation Assessment is to determine if any of the ongoing activities have an impact to 'us' or if they can have (in the future) an impact to 'us'. The first part looks at the current activities and assessing the impact that the activities have had. Since these activities have already happened, we refer to this as "Damage" Assessment,

i.e., has any of the identified activities caused a current impact and specifically has it caused harm that requires development of a recovery plan to resolve the condition(s) that the activity has generated. In order to accomplish this type of assessment, one not only needs the current, known activities, but also what each activity means to "us" (i.e., Does the given activity impact us in some way?). The data needed to perform this analysis is part of what we call "Knowledge of Us". Thus, this part of the process identifies to the decision maker whether there is a current impact to any of his/her capabilities or assets and whether there is an impact in his/her ability to perform the mission.

Above, we discussed the current situation and assessing the situation including its impact to the mission, but a decision maker may also be interested in a view of what the adversary (or competitor) is doing or may possibly do. This has generally been described as "getting inside the adversary's OODA loop". The sooner we understand what the adversary can/might do the more options become available to the decision maker. The second part of Figure 2 addresses this. The first step of the process is to take each AOI and project it forward based on the a priori knowledge provided as part of the model. Here we don't discuss time itself, i.e., we are not projecting the activities based on time, but rather the next step in the process. In some cases it could take milliseconds to go from one stage to another and in other cases it could be days, or longer. The number of stages that we look forward is defined under "Configuration Data". Based solely on the models themselves, we have projected each current activity one or more steps forward; however, these projected or possible futures do not take into account whether they are plausible. In order to determine plausibility, we need to consider additional knowledge. We need both the Knowledge of "Them" and Knowledge of "Us". Specifically, we need to know whether the adversary has the capability, capacity, intent/goal, and have they exhibited similar behavior in the past. We also need to know whether they have the opportunity to accomplish the intent(s)/goal(s).

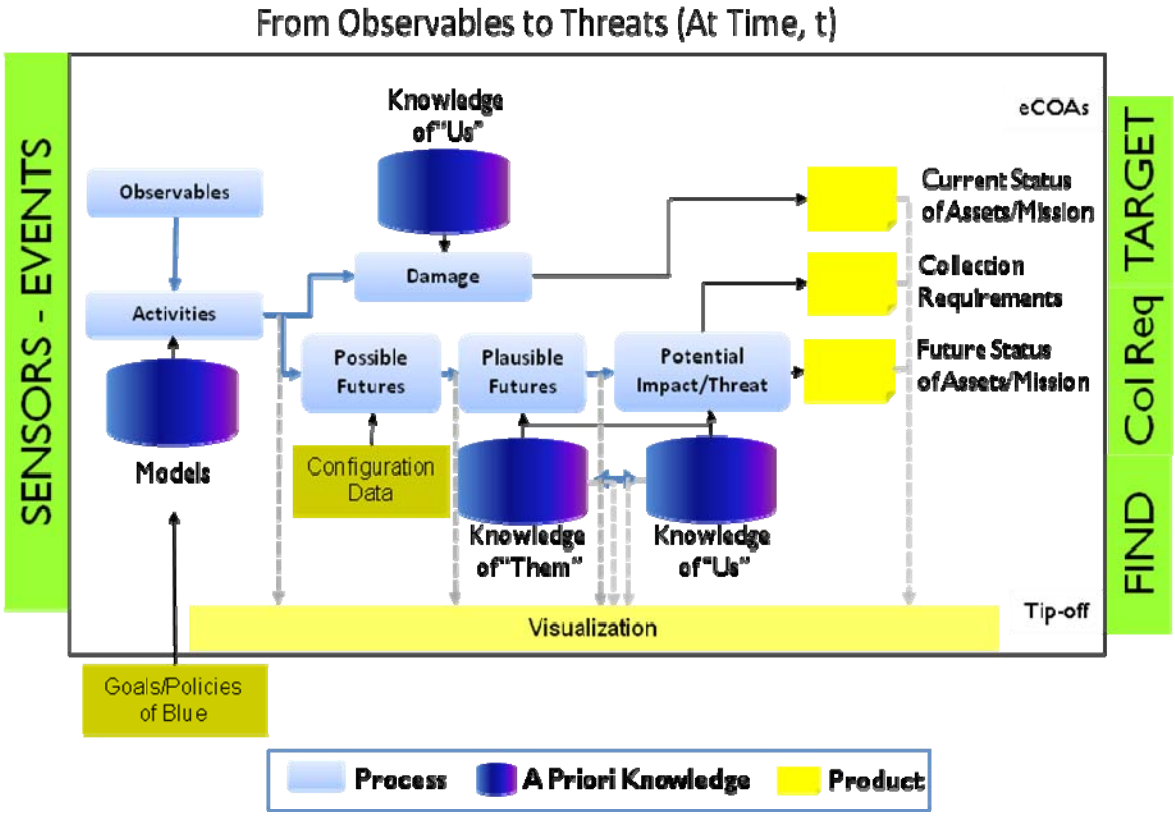

Figure 2 - Situation Awareness Process Model

This opportunity is based in many cases on the vulnerabilities of us (provided as part of the Knowledge of "Us"). Thus, starting with the list of possible futures, we use the Knowledge of "Them" and Knowledge of "Us" to constrain the possible into the plausible for each activity of interest. But again what

do these plausible futures mean to me/us? To answer this question we again use part of the Knowledge of "Us" (importance of the assets/capabilities) to identify potential impacts and threats to meeting our objective(s). From this portion of the process we get not only future potential impacts/threats but we can also use this knowledge to determine our future collection requirements. Based on each of the futures, we can identify the key differentiating events that will assist us in determining which of the plausible futures may actually be unfolding. The key differentiating events can then determine the collection requirements needed to increase the certainty in identifying whether a plausible future is occurring. One of the dangers in a reference model such as the one in Figure 1 is that it can be perceived as a sequential flow of data or information rather than a descriptive model of components and ideas. To help circumvent this danger, Figure 2 attempts to define a process flow and end products that is based on the concepts of the reference model as its framework. A primary feature of the process model is that it defines components that can be implemented as automated computer applications or shared human/computer systems that can then be tied together within system architectures. It also describes the flow of information and when key data sources come into play.

3. Conclusion

This paper has described a reference model and a flow or thread through it for a given time, t. The SA Reference Model provides a set of definitions that can serve as a reference for describing systems that aid with SA while the Process Model captures a process flow at a single point in time. Together, the two models provide a common set of definitions for situation awareness. The goal in presenting the reference model and process thread was to describe how one can identify significant activities of interest or of concern to oneself and to one's goals/objectives. In doing so, the hope is to be able to focus the analyst's attention onto what is important, thus minimizing the current the work overload and maximizing the decision maker's situation awareness. Products include plausible adversarial futures ranked based on threat (Most "Dangerous" and Most "Likely" and generally refer to as enemy Courses of Actions, eCOA), a list of collection requirements and possible tip offs based on differentiating events and anticipated futures.

4. References

1. M. Endsley, March 1995. *Toward a Theory of Situation Awareness in Dynamic Systems*. In Human Factors Journal, Volume 37(1), pages 32-64, March 1995.
2. J. Salerno, G. Tadda, D. Boulware, M. Hinman and S. Gorton, "Achieving Situation Awareness in a Cyber Environment", In Proc of the Situation Management Workshop of MILCOM 2005, Atlantic City, NJ, October 2005.
3. U.S. Department of Defense, Data Fusion Subpanel for the Joint directors of Laboratories, Technical Panel for C3, "Data Fusion Lexicon," 1991.
4. A. Steinberg, C. Bowman, and F. White. Revisions to the JDL Data Fusion Model, presented at the Joint NATO/IRIS Conference, Quebec. October 1998.
5. J. Salerno, M. Hinman, and D. Boulware, *A Situation Awareness Model Applied to Multiple Domains*. Proceedings of the Defense and Security Conference, Orlando FL, March 2005.
6. J. Salerno, M. Hinman, and D. Boulware, *Evaluating Algorithmic Techniques in Supporting Situation Awareness*, Proceedings of the Defense and Security Conference, Orlando FL, March 2005.
7. J. Salerno, *Measuring Situation Assessment Performance through the Activities of Interest Score*, Proceedings of the 11th International Conference on Information Fusion, Cologne GE, June 30 – July 3, 2008.
8. G. Tadda, et al., *Realizing Situation Awareness within a Cyber Environment*. In Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006, edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 6242 (SPIE, Bellingham, WA, 2006) 624204, Kissimmee FL, April 2006.
9. G. Tadda, *Measuring Performance of Cyber Situation Awareness Systems*, Proceedings of the 11th International Conference on Information Fusion, Cologne GE, June 30 – July 3, 2008.
10. E. Bosse, J. Roy, and S. Wark, "Concepts, Models, and Tools for Information Fusion", Artech House, Inc., 2007, ISBN-13: 978-1-59693-081-0, pg 4.
11. Alan N. Steinberg, "Foundations of Situation and Threat Assessment", Chapter 18 of Handbook of Multisensor Data Fusion, ed. Martin E. Liggins, David L. Hall and James Llinas, CRC Press, London, 2009.